Domácí úkol z 9. listopadu 2017

Rovnicí $Y^2 = X^3 - 2X$ je zadána eliptická křivka E nad třináctiprvkovým tělesem $\mathbb{Z}_{13}$.

1. Ukažte, že body $A = (-1, 1)$ a $B = (-4, 3)$ leží na E a mají zde řád 3.
2. Na eliptické křivce E spočítejte hodnotu Weilova párování $e_3(A, B)$.

[Návod: výhodnější než přímý výpočet z definice Weilova párování je užít větu 11.12, která je ve Washingtonově knize na straně 359.]